22

IDENTITY THEFT

§22.1 Introduction

This consumer rights chapter describes ways to frustrate identity thieves and the steps you should take if your identity has been stolen.[1] Both in Maine and nationally, identity theft is the most common consumer complaint.[2] If your identity has been stolen, you must act quickly to limit your losses. Follow the steps described below and keep good records.

§22.2. How to Keep Your Identity Safe

Your date of birth, name and Social Security number are all the information a thief needs to steal your identity. If you are contacted by phone, mail or e-mail and asked to provide any of these, first ask yourself: "Would I give the key to my home, the key to my vehicle or my checkbook to this person?" If the answer to any of these of questions is "No"—don't provide the information. And remember: legitimate companies never ask for personal financial information over the internet.

You can deter identity thieves by safeguarding your information in the following ways:

A. Shred financial documents and paperwork with personal information before you discard them.

B. Protect your Social Security number. Don't carry your Social Security card in your wallet or write your Social Security number on a check. Give it out only if absolutely necessary or ask to use another identifier.

---

[1] This chapter was written by Jane Carpenter, Maine Attorney General Assistant Complaint Examiner. For additional identity theft information to to Federal Trade Commission (www.ftc.gov/bcp/edu).

[2] In Maine, ID theft now tops the list of our most common consumer complaints:

1. Identity Theft
2. Home Construction
3. TV, Audio, Video Equipment
4. Used Motor Vehicles
5. Motor Vehicle Repairs
6. New Motor Vehicles
7. Cable/Satellite TV
8. Wireless Telephone
9. Housing, Real Estate, Rentals.

C. Don't give out personal information on the phone, through the mail or over the Internet unless you know exactly who you are dealing with.

D. Never click on links sent in unsolicited e-mails; instead, type in a web address you know. Use firewalls, anti-spyware, and anti-virus software to protect your home computer; keep them up to date. Visit www.OnGuardOnline.gov for more information.

E. Don't use obvious passwords like your birthday, your mother's maiden name, or the last four digits of your Social Security number.

F. Keep your personal information in a secure place at home, especially if you have roommates, employ outside help, or are having work done in your house.

G. Be cautious with your mail. Don't leave mail in your mailbox or where strangers may have access to it. Don't include personal financial information or Social Security numbers in your e-mails. You can add your name to the Direct Marketing Association's "Do Not Mail" list by calling them at 212-790-1500, writing to them at 615 L Street NW, Suite 1100, Washington, DC 20036-3603, or registering on their website at http://www.dmaconsumers.org/consumerassistance.html.

§22.3. How to Detect Identity theft

The best way to detect suspicious activity is by regularly checking your credit reports and billing statements. Be alert to signs that require immediate attention:

A. Bills that do not arrive as expected;

B. Unexpected credit card or account statements;

C. Denials of credit for no apparent reason; and

D. Calls or letters about purchases you did not make.

It is also very important to periodically inspect your credit report. Your credit report contains records of your bill paying history. State and federal law requires each of the major nationwide consumer reporting agencies—Equifax, Experian, and TransUnion—to give you a free copy of your credit report once a year if you ask for it. Go to www.annualcreditreport.com or call 1-877-322-8228, a service created by these three agencies, to order your free credit reports each year. You can also write: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. *See* §22.6, How to Read Your Credit Report.

Finally, and also very important, you should review your financial accounts and billing statements regularly, looking for charges you did not make. This is perhaps the most effective way to detect identity theft. You must also be aware of the latest internet scams designed to steal your identity. Remember, a bank never uses e-mails to contact you. Basically, never open an e-mail link unless you personally know the person who sent it to you. Just by opening a link, thieves can plant spyware, Trojan horses and viruses. And it's always a scam when an e-mail, letter or phone call tells you that you have won a prize but that you have to pay money to get it. It's a scam.

§22.4 What To Do If Your Identity Has Been Stolen

If you believe you have become a victim of identity theft, you must act immediately to minimize the damage and to secure your legal rights. Fighting identity theft can be frustrating and time-consuming, but resources exist to help you. Here are the steps you should follow.

A. Place A Fraud Alert: Contact Any Of The Three Consumer Reporting Agencies

Your first step is to place a fraud alert on your credit report. Contact any one of the three credit reporting agencies:

(1) Equifax: 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241

(2) Experian: 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9532, Allen, TX 75013

(3) TransUnion: 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

Contacting one of the three agencies above automatically alerts the other two agencies which will also place an alert in their records.

When you call, an initial fraud alert (90 days) will be placed on your credit report and a free copy of your credit report will be sent to you. (This does not count as your one free copy per year.) The fraud alert lets potential creditors know that there may be a problem with your credit information and should prevent new accounts from being opened in your name without permission. After the initial fraud alert has expired, if you have filed a police report, you can request an extended fraud alert (7 years.) To obtain an extended fraud alert, you must provide the credit reporting companies with a copy of your initial police report and any other fraud reports they may require. There is no charge for a fraud alert.[3]

As of February, 2006, Maine became one of several states to allow consumers to "freeze" their credit reports. With certain specific exceptions, a security freeze prohibits a credit reporting agency from releasing your credit report or any information from it without your express authorization. This shall prevent crooks from using your credit record to open false new accounts because most businesses will not open new accounts without first checking the applicant's credit history. The freeze goes into effect five (5) business days after the credit reporting agency has received your request. After 10 business days from receiving your letter to place a freeze on your account, the credit reporting agency will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep this PIN or password in a safe place. If your credit files are frozen, even someone who has your name and Social Security number probably would not be able to obtain credit in your name. A security freeze is free to identity theft victims who have a police report, investigative report or a complaint to a law enforcement agency concerning identity theft. However, there is a charge every time the freeze is lifted to release your credit information.

See §22.8(A) for a sample letter requesting a security freeze. Credit reporting agencies charge a $10 fee, unless you are a victim who sends a copy of your police report, investigative report or a complaint to a law enforcement agency concerning identity theft.

[3] Members of the military who are on active duty can place a military fraud alert even if they have not been a victim of identity theft.

B. Report The Crime Immediately To Local Law Enforcement

Make sure a written report is taken and that you receive a copy of the Police Report so that you can give copies to creditors. Effective July, 2008 Maine law enforcement are required to accept your identity theft report and provide you with a copy of it. *See* 10 M.R.S.A. §1350-B. If you have difficulty obtaining a copy of your report, contact the Attorney General at 626-8800. See §22.5, Identity Theft Police Report.

C. Contact Any Creditors Or Financial Institutions If You Believe Your Accounts Have Been Tampered With Or If Fraudulent Accounts Have Been Opened

Close your accounts and ask for a fraud investigation. If you contact them initially by phone, make sure that you confirm your conversation in writing. *See* §22.8(B) for a sample letter disputing a fraudulent account or charge. Some companies have forms you can use to dispute the charges due to fraud. *In most cases, to limit your financial responsibility, your dispute of charges must take place within sixty days of the initial fraud.*

Under the Fair Credit Reporting Act (FCRA), both the credit reporting agency and the information provider (the business that sent the information to the credit reporting company), such as a bank or credit card company, are responsible for correcting fraudulent information in your report. To protect your rights under the law, contact both the credit reporting agency and the information provider.

D. Steps to Take If The Identity Theft Has Resulted In A Fraudulent Electronic Withdrawal From Your Account

Here are ways to respond to a fraudulent electronic withdrawal from one of your accounts:

(1) The Electronic Fund Transfer Act provides consumer protections for transactions involving an ATM or debit card, or other electronic ways to debit or credit an account. It also limits your liability for unauthorized electronic fund transfers.

(2) You have 60 days from the date your bank account statement is sent to you to report in writing any money withdrawn from your account without your permission. This includes instances when your ATM or debit card is "skimmed" that is, when a thief captures your account number and PIN without your card having been lost or stolen.

(3) If your ATM or debit card is lost or stolen, report it immediately because the amount you can be held responsible for depends on how quickly you report the loss.

(4) If you report the loss or theft within two business days of discovery, your losses are limited to $50.

(5) If you report the loss or theft after two business days, but within 60 days after the unauthorized electronic fund transfer appears on your statement, you could lose up to $500 of what the thief withdraws.

(6) If you wait more than 60 days to report the loss or theft, you could lose all the money that was taken from your account after the end of the 60 days.

(7) Note: VISA and MasterCard voluntarily have agreed to limit consumers' liability for unauthorized use of their debit cards in most instances to $50 per card, no matter how much time has elapsed since the discovery of the loss or theft of the card.

The best way to protect yourself in the event of an error or fraudulent transaction is to call the financial institution and follow up in writing by certified letter, return receipt requested so you can prove when the institution received your letter. Keep a copy of the letter you send for your records.

After receiving your notification about an error on your statement, the institution generally has 10 business days to investigate. The institution must tell you the results of its investigation within three business days after completing it and must correct an error within one business day after determining that it occurred. If the institution needs more time, it may take up to 45 days to complete the investigation but only if the money in dispute is returned to your account and you are notified promptly of the credit. At the end of the investigation, if no error has been found, the institution may take the money back if it sends you a written explanation.

E. Steps To Take If The Identity Theft Has Occurred Due To A Fraudulent Check Or Other "Paper" Transaction

In general, if an identity thief steals your checks or counterfeits checks from your existing bank account, you must notify the bank to stop payment, close the account, and ask your bank to notify Chex Systems, Inc. or the check verification service with which it does business. That way, retailers can be notified not to accept these checks. While no federal law limits your losses if someone uses your checks with a forged signature, or uses another type of "paper" transaction such as a demand draft, Maine law offers protection. Under Maine's Uniform Commercial Code if someone forges your name on one of your checks it should not be regarded as properly payable and should not be charged to your account. Thus, the bank should be responsible for losses from such transactions. At the same time, you should take reasonable care of your account. For example, you may be held responsible for the forgery if you fail to notify the bank in a timely manner that a check was lost or stolen. Contact the Maine Bureau of Financial Institutions (1-800-965-5235 or 207-624-8570 for more information.

You can contact major check verification companies directly for the following services:

(1) To request that they notify retailers who use their databases not to accept your checks, call: TeleCheck at 1-800-710-9898 or 1-800-927-0188; Certegy, Inc. (previously Equifax Check Systems) at 1-800-437-5120.

(2) To find out if the identity thief has been passing bad checks in your name, call SCAN: 1-800-262-7771.

If your checks are rejected by a merchant, it may be because an identity thief is using the Magnetic Information Character Recognition (MICR) code (the numbers at the bottom of checks), your driver's license number, or another identification number. The merchant who rejects your check should give you its check verification company contact information so you can find out what type of information the thief is using.

If you find that the thief is using your MICR code, ask your bank to close your checking account and open a new one. If you discover that the thief is using your driver's license number or some other identification number, work with the Bureau of Motor Vehicles or other identification issuing agency to get new identification with new numbers. Once you have taken the appropriate steps, your checks should be accepted. The check verification company may or may not remove the information about the MICR code or the driver's license/identification number from its database because this information may help prevent the thief from continuing to commit fraud. If the checks are being passed on a new account, contact the bank to close the account. Also contact Chex Systems, Inc., to review your consumer report to make sure that no other bank accounts have been opened in your name. Dispute any bad checks passed in your name with merchants so they don't start any collection actions against you.

F. File A Report With The Federal Trade Commission (FTC)

You can file a report by visiting https://rn.ftc.gov/pls/dod/widtpubl$.startup?Z_ORG_CODE=PU03. To find out more about your rights, specific laws and sample forms(including a sample Identity Theft Affidavit), visit http://www.ftc.gov/bcp/edu/microsites/idtheft/

G. Contact The 3 Credit Reporting Agencies Using The Form They Provide To Correct Errors And Place A Block On The Accounts In Question.

Once you have received a copy of your Credit Report, review it carefully for errors and make sure they are fixed.

The Fair Credit Reporting Act mandates that credit reporting agencies must remove the incorrect information unless the credit issuer can prove that it is true. The credit reporting agencies must also change any information provided by the thief including addresses, phone numbers or birthdates. See §22.8(c) for a sample letter to correct errors in your credit report.

To dispute an error on your credit report you need to create a paper trail. Keep copies of all documents you send or receive from the credit agency or the lender and the names and phone numbers of people who contacted you about your dispute. Contact the credit reporting agency and the lender who provided the inaccurate information (if it is clear where that information came from) to dispute the claim in writing.

Send your dispute letter by certified mail so you have proof that the letter was received. You can also dispute the error online on the websites of the three credit-reporting agencies, but if you decide to do this, be sure to print the claim for your records. By law, the agency has just 30 days to respond to your request to fix the error, and they must notify other credit reporting agencies of the correction if the error has dented your score. If you don't like the response you get from the credit-reporting agency, you can mail the agency a letter explaining your side of the story and ask that your letter be permanently attached to your file.

H. Use An ID Theft Police Report (§22.5) And Insist On Clearance Letters From The Creditors And/Or Credit Reporting Companies And Keep Them In Your Records For 10 Years.

I. Carefully Check All Credit Reports To Make Sure The Corrections Have Been Made.

J. Additional Resources

(1) **Maine Attorney General Consumer Protection Division:** 207-626-8849, or visit consumer.mediation@maine.gov;

(2) **Maine Office of Consumer Credit Regulation:** (207) 624-8527 Toll Free consumer line (Maine only) 1-800-332-8529, 35 State House Station, Augusta, Maine 04330-0035;

(3) **Maine Bureau of Motor Vehicles** (to report stolen driver's license): 207-624-9000 extension 52144, write to 29 State House Station Augusta, Maine 04333 or visit the website at http://www.maine.gov/sos/bmv/index.html;

(4) **Federal Do Not Call Registry**: You can register online at www.donotcall.gov or call toll-free, 1-888-382-1222 from the number you wish to register;

(5) **Federal Trade Commission Hotline** (1-877-ID-THEFT);

(6) **Tax Fraud:** IRS Taxpayer Advocate Service www.irs.gov/advocate/ or call toll-free: 1-877-777-4778;

(7) **Social Security Administration (SSA) Office of the Inspector General**: You may file a complaint online at www.socialsecurity.gov/oig, call toll-free: 1-800-269-0271, fax: 410-597-0118, or write: SSA Fraud Hotline, P.O. Box 17768, Baltimore, MD 21235;

(8) **Maine Bureau of Financial Institutions** (for banking questions): 1-800-965-5235 or 207-624-8570;

(9) **Phone Fraud:**

(a) **For non-cellular phones**, call the Maine Public Utilities Commission Consumer Assistance Hotline at 1-800-452-4699.

(b) **For cellular phones and long distance**, contact the Federal Communications Commission (FCC) at www.fcc.gov. The FCC regulates interstate and international communications by radio, television, wire, satellite, and cable. Call: 1-888-CALL-FCC; TTY: 1-888-TELL-FCC; or write: Federal Communications Commission, Consumer Information Bureau, 445 12th Street, SW, Room 5A863, Washington, DC 20554. You can file complaints online at www.fcc.gov, or e-mail your questions to fccinfo@fcc.gov.

(c) **Mail Theft** - The U.S. Postal Inspection Service (USPIS) is the law enforcement arm of the U.S. Postal Service and investigates cases of identity theft. The USPIS has primary jurisdiction in all matters infringing on the integrity of the U.S. mail. If an identity thief has stolen your mail to get new credit cards, bank or credit card statements, pre-screened credit offers, or tax information, or has falsified change-of-address forms or obtained your personal information through a fraud conducted by mail, report it by calling the U. S. Postal Inspector at 207-871-8587 or by writing: U. S. Postal Inspector, State of Maine, 125 Forest Avenue, Portland, ME 04104.

§22.5. Identity Theft Police Report

An Identity Theft Police Report is a police report with more than the usual amount of detail. The Identity Theft Report includes enough detail about the crime for the credit reporting companies and the

businesses involved to verify that you are a victim—and to know which accounts and inaccurate information came from identity theft. Normal police reports often do not have many details about the accounts that were opened or misused by identity thieves. Maine law requires the local police department to make a report of your identity theft and provide you with a copy (10 M.R.S.A. §1350-B). For additional information, go to ftc.gov or call 1-877-10-THEFT.

Creating and using an Identity Theft Report may require two steps:

A. Step one is to file your report with local law enforcement or the Attorney General's Office. In your report you should give as much information as you can about the crime, including anything you know about the dates of the identity theft, the fraudulent accounts opened and the alleged identity thief.

B. Step two begins when you send the business involved and the credit reporting companies a copy of the Identity Theft Police Report, which you should do by certified mail, return receipt requested. The companies may ask you to give them more information or documentation to help them verify your identity theft. They have to make the request within 15 days of receiving your Identity Theft Report. The credit reporting company or business then has 15 more days to work with you to make sure your Identity Theft Report contains everything they need. They are also entitled to 5 days to review the information you give them. For example, if you give them information 11 days after they request it, they have until day 16 to make a final decision.

When you send a copy of your Identity Theft Report to the fraud departments of the three major credit reporting companies, include a copy of the credit reporting company cover letter, along with copies of your supporting documentation. For a sample letter, *see* §22.8(C).

If you have trouble obtaining an Identity Theft Police Report, contact the Maine Attorney General for assistance (207-626-8849 or consumer.mediation@maine.gov).

§22.6. How To Read Your Credit Report

One way to guard against identity theft is to carefully read your Credit Report. But Credit Reports are often very difficult to read. Nonetheless, it is an extremely valuable document. It reflects your entire financial life. The *Wall Street Journal* offers the following advice about reading your Credit Report:

A. The first section includes **personal information** specific to you. It is very common to find errors—and occasionally fraudulent information—in this section. Don't panic: it is not unusual to find that your name has been misspelled or that many variations of your name appear. Credit-reporting companies rely on information provided by your creditors, and often something gets lost in the translation. But there is cause for alarm if you discover an entirely different name, address or driver's license number on your file. These are a few red flags for possible identity theft.

B. The next section is your **credit history**. Here you will find a line-by-line description of every creditor account that has been reported. These entries include the name of the lender and account number, when it was opened and other relevant information, including whether the account when into collection or was written off by the creditor. You will want to spend some time looking over this section carefully. For example, people with very common surnames sometimes find that someone else's account information appears on their credit report. It happens most often within families—a father's mortgage might appear in his college age son's credit report because they share the same name.

C. While most people believe that your credit (borrowing) history contains the

information that is most harmful to their credit scores, the real damage happens in the next section: **public records**. Here you will find public filings on such things as past judgments, liens and bankruptcy-protection filings. If you have ever been convicted of a criminal activity, such as drunken driving, your record very well might show up here, too.

D. Finally, the "**inquiries**" section of your credit report lists the types of companies that have requested information about you. There are two types of inquiries: hard and soft. Whenever you do such things as request a copy of your own credit report, apply for a credit card or sign up for a new cell phone plan, it is considered a hard inquiry. Soft inquiries, on the other hand, are initiated by companies that want to sell you something, such as a new rewards credit card or preapproved line of credit.

§22.7. Summary: Your Identity Theft Rights

As identity theft has exploded over the last three years, Maine and federal laws have given consumers specific additional rights. Here is a brief summary of these rights:

A. Identity Theft Reports

You have a right to receive from a law enforcement agency (your local police department or the Maine Attorney General's Office) an Identity Theft Police Report (10 M.R.S.A. §1350-B). This is a Police Report with enough information about the crime that the credit reporting companies and the businesses involved can verify that you are a victim, and know which accounts and information have been affected. This is the report that will give you access to many of the rights described here.

B. When It Comes To Credit Reporting Companies You Have The Following Rights:

(1) Place a 90 day Initial Fraud Alert or a security freeze on your credit files. The fraud alert tells users of your credit report that they must take reasonable steps to verify who is applying for credit in your name. To place a 90 day fraud alert, contact one of the three nationwide credit reporting companies. The one you contact has to notify the other two. A security freeze will prevent creditors from accessing your credit report at all, unless you lift the freeze or you already have a business relationship with the company.

(2) Place a seven-year Extended Fraud Alert on your credit files. You would do this if you know you are a victim of identity theft. You will need to give an Identity Theft Police Report to each of the credit reporting companies. Each reporting company will ask you to give them some way for potential creditors to reach you, like a phone number. They will place this contact information on the Extended Fraud Alert as a signal to those who use your credit report that they must contact you before they can issue credit in your name.

(3) Get a free copy of your credit report and a summary of your rights from each credit reporting company. You can get these when you place a 90-day Initial Fraud Alert on your credit reports. When you place an Extended Fraud Alert with any credit reporting company, you have the right to two copies of that credit report during a twelve month period. These credit reports are in addition to the free credit report that all consumers are entitled to each year.

(4) Ask the credit reporting companies to block fraudulent information from appearing on your credit report. To do this, you must submit a copy of a valid Identity Theft Police Report. The credit reporting companies then must tell any creditors who gave them fraudulent information that it resulted from identity theft. The creditors may not then turn the fraudulent debts over to debt collectors.

(5) Dispute fraudulent or inaccurate information on your credit report with a credit reporting company.

C. Dealing With Creditors, Debt Collectors and Merchants.

(1) You have a right to have a credit report free of fraudulent accounts. Once you give creditors and debt collectors a copy of a valid Identity Theft Police Report, they may not report fraudulent accounts to the credit reporting companies.

(2) You have a right to get copies of documents related to the theft of your identity—for example, applications used to open new accounts or transaction records—if you give the company a valid Police Report. You can also tell the company to give the documents to a specific law enforcement agency; that agency doesn't have to get a subpoena for the records.

(3) You have a right to stop the collection of fraudulent debts. You may ask debt collectors to stop contacting you to collect on fraudulent debts. You also may ask them to give you information related to the debt, like the names of the creditors and the amounts of the debts.

D. Limiting Your Loss From Identity Theft.

(1) Fraudulent credit card charges: You cannot be held liable for more than $50 for fraudulent purchases made with your credit card, as long as you let the credit card company know within 60 days of when the credit card statement with the fraudulent charges was sent to you. Some credit card issuers say card holders who are victims of fraudulent transactions on their accounts have no liability for them at all.

(2) Lost or stolen ATM/Debit Cards: If your ATM or Debit card is lost or stolen, you may not be held liable for more than $50 for the misuse of your card, as long as you notify the bank or credit union within two business days after you realize the card is missing. If you do not report the loss of your card promptly, your liability may increase.

(3) Fraudulent electronic withdrawals: If fraudulent electronic withdrawals are made from your bank or credit union account, and your ATM or Debit card has not been lost or stolen, you are not liable, as long as you notify the bank or credit union in writing of the error within 60 days of the date the bank or credit union account statement with the fraudulent withdrawals was sent to you.

(4) Fraudulent Checks: Under most state laws, you are liable for just a limited amount for fraudulent checks issued on your bank or credit union account, as long as you notify the bank or credit union promptly. Contact the Maine Bureau of Financial Institutions for more information.

(5) You are not liable for any debt incurred on fraudulent accounts opened in your name and without your permission.

E. Right To Be Notified If Your Financial Records Have Been Stolen Or Lost.

Maine Law (10 M.R.S.A. §1348) requires a business which maintains computerized data that includes personal information[4] to notify consumers whenever that information has been compromised or stolen. This notice of a data breach[5] must be made "as expediently as possible and without unreasonable delay...." Here is a March, 2008 example of such a notice:

> We regret to inform you about an incident that may have put personal information of some residents of Maine at some degree of risk. In late February, a 3M employee's laptop was stolen from a parked car. We believe that there was a file on this laptop that contained names and social security numbers for approximately 9 residents of Maine. Because this appears to be a crime of opportunity, police believe there is a low risk that this information would be misused. We are contacting you so you are aware of the situation as required by your state law.

[4] "Personal information" means your first name, or first initial, and last name in combination with any one or more of the following:

1. Your social security number;
2. Your driver's license number or state identification card number;
3. Your account number, credit card number or debit card number, if circumstances exist where the number cour be used without additional identifying information;
4. Your account passwords or personal identification numbers or other access codes; or
5. Any of the above when not used in connection with your first name, or first initial, and last name, if the information would be sufficient to permit someone to attempt or commit identity theft.

[5] Under 10 M.R.S.A., §1347, a data breach means that someone without authorization has acquired your personal information and by doing so has compromised the security of your information. It is not a data breach if your information was acquired by someone acting as an employee or agent of the organization if the information is not subject to further disclosure.

F. What Should You Do If You Have Been A Victim Of A Data Breach?

What should you do if you learn that the confidentiality of your personal financial information has been breached? Many people first find out through a news report or a notification letter from a business or organization. If your information has fallen into the hands of an unauthorized person, it does not mean that you have become a victim of identity theft. A data breach does not necessarily result I an identity theft. Identity theft does not occur until an unauthorized person fraudulently uses your information to secure money, goods or services in your name. The following information may be helpful to you in protecting yourself if you discover you have been the victim of a data breach:

(1) Immediately contact one of the three credit reporting agencies at the toll free phone numbers shown below to place a Fraud Alert on your credit report. The first agency you contact will notify the other two agencies on your behalf. The process is automated and you will need to provide your social security number in order to place the Fraud Alert. We suggest that you do not use the internet to place your Fraud Alert. The Fraud Alert will remain in effect for 90 days after which time you may extend the alert. By placing the Fraud Alert on your credit report creditors will be notified if someone attempts to use your information to open new accounts or apply for a loan.

Transunion:	**1-800-680-7289**	**TDD:**	**1-877-553-7803**
Equifax:	**1-800-525-6285**	**TDD:**	**1-800-255-0056**
Experian:	**1-888-397-3742**	**TDD:**	**1-800-397-3742**

(2) As a resident of Maine, you may also place a Security Freeze or "File Freeze" on your credit report at a cost of no more than $10 for each freeze or removal of a freeze. There is an additional charge to suspend the freeze for a specific inquiry. With a Security Freeze in place, your information may not be released without your authorization. Once you have sent the agency a written request by certified mail, the agency must send you confirmation of the freeze within 10 business days. At that time, they will also send you an identification number or password that you can use if you want your information provided to a business or organization.

(3) If information about your financial accounts was stolen, immediately close the accounts. If the theft includes your driver's license or other form of identification that was issued by a government agency, contact the issuing agency and request a replacement. Ask if the agency will flag your information to prevent someone else from using your information. For more information please contact the Office of the Attorney General at 1-800-436-2131.

G. Beware of Medical ID Theft

An increasing problem is medical-ID theft. One reported case involved a clinic in Florida. A clerk stole more than a thousand patient records and with the help of her cousin submitted more than 2.5 million dollars of false claims to Medicare. This type of theft is very hard to prevent. But you can make sure you do not end up paying for procedures you never received. One suggestion is to look at your bills for your last three doctor visits. A fake charge should be a red flag. You should also ask for an annual statement of benefits from your insurer.

§22.8. Sample Identity Theft Letters

Here are several sample letters you can use in enforcing your identity theft rights.

A. Security Freeze Letter To Credit Reporting Company:

Here is a sample letter which you can use to write to a credit reporting company to ask it to put a Security Freeze on your account:

Date:

Credit Reporting Company and Address:

Dear _____:

I would like to place a security freeze on my credit file. Here is my personal information:
Current Name: _____
Former Name (if applies):_____
My current address is: _____
My address has changed in the past five years. My former address was:
_____
My Social Security Number is:_____
My Date of Birth is: _____

Circle One:

I have included my payment of $10 to freeze my credit file.

OR

I am an identity theft victim and a copy of my police report (or other investigative report or complaint to a law enforcement agency concerning identity theft) of identity theft is enclosed.

Yours Truly,

Your Name, Address and Contact Information

B. Dispute Letter For Existing Accounts.

Here is a sample letter that you can use that you can use when you dispute a fraudulent account or charge due to identity theft:

Date

Name of Creditor
Billing Inquiries
Address
City, State Zip Code

Dear Sir or Madam:

I am writing to dispute a fraudulent (charge or debit) on my account in the amount of $_____. My account # is: _____. I am a victim of identity theft, and I did not make this (charge or debit). I am requesting that the (charge be removed or the debit reinstated), that any finance and other charges related to the fraudulent amount be credited, and that I receive an accurate statement.

Enclosed are copies of (use this sentence to describe any enclosed information, such as a Police Report) supporting my position. Please investigate this matter and correct the fraudulent (charge or debit) as soon as possible.

Sincerely,

Your Name
Your Address
Your City, State, Zip Code
Your Account Number

Enclosures: (List what you are enclosing.)

C. Blocking Letter to Credit Reporting Companies

Here is a sample letter to the three credit reporting companies requesting that they correct errors and place a block on the accounts in question:

Date

Complaint Department
Name of Consumer Reporting Company
Address
City, State, Zip Code

Dear Sir or Madam:

I am a victim of identity theft. I am writing to request that you block the following fraudulent information in my file. This information does not relate to any transaction that I have made. The items also are circled on the attached copy of the Credit Report I received. (Identify item(s) to be blocked by name of source, such as creditors or tax court, and identify type of item, such as credit account, judgment, etc.)

Enclosed is a copy of the Identity Theft Police Report regarding my identity theft. Please let me know if you need any other information from me to block this information on my credit report.

Sincerely,

Your Name
Your Address
Your City, State, Zip Code

Enclosures: (List what you are enclosing.)